

# Securing IBM Lotus Sametime

## What is Sametime?

IBM® Lotus® Sametime® software is a client-server application that provides enterprise-level, real-time communication services through voice, video and data integration. It is a key component of IBM's Unified Communication and Collaboration (UC<sup>2</sup><sup>™</sup>) solutions. Some of its most notable features include online meetings, voice and video conferencing, telephony, mobility integration, enterprise instant messaging (IM), community collaboration and overall presence awareness.

## Why should you secure Sametime?

A fully implemented Sametime solution can be an extremely powerful tool for an organization. With the ability to link your desktop computer, desk phone, notebook computer, and cell phone, employees can collaborate anywhere, anytime. Colleagues can communicate and work face-to-face regardless of where they are physically. It can also be extended outside the enterprise and used to connect to other Sametime communities, as well as third-party IM solutions.

Sametime can easily become the nerve center of an organization. As information is allowed to flow freely between all the enterprise communication channels, protecting that information becomes ever more challenging and critical. Now, a seemingly innocuous desktop computer compromise potentially exposes email, phone lines, web conferences, IM conversations, and even associated cell phones to that same threat. The systems that were once isolated from each other are now interconnected, thus vastly increasing the attack surface.

## So, how do you protect yourself?

Any solution that is deployed in an organization is only as strong as the system it is installed on, and in turn only as strong as the network that connects it. A layered methodology to enterprise security, or “defense in depth,” is a common approach to ensure attack surface reduction and to secure an environment.

### Strong passwords

All Sametime users should have passwords that are not easily guessable. Policies should be implemented to enforce password length and complexity in accordance with corporate guidelines. Administrator accounts should always have more complex password requirements than regular user accounts.

### Configure SSL

Strong passwords are of little use if the credentials are sent across the network unencrypted. Although many of Sametime's components take advantage of the native encryption built into the software, some features rely on external encryption. The web conferencing component in Sametime is one part that depends on encryption from the web server. In order to better protect connections and data in a web conference, it is imperative to have strong SSL encryption enabled on the web server hosting the Sametime software. In addition, all connections made to the HTTP site should be automatically redirected to HTTPS.



The Information Assurance Mission at NSA

## Anonymous Access?

If there is not a business need for anonymous access to the Sametime environment, it should be disabled altogether. Access to network resources and other systems that integrate with Sametime typically require authentication, so anonymous access may not provide adequate permissions for collaboration. However, if anonymous access is desired, then it is important to ensure that it is explicitly denied permissions to parts of the environment that are not necessary. This especially includes access to critical Sametime databases. An alternative for users who need short-term access to the system may be to create temporary accounts that have very limited access and can be enabled and disabled as needed.

## Latest and greatest

In addition to applying the latest patches and security updates to Sametime, all web components should be accessed using the latest web browser. Use of the newest web browsers will provide Sametime users with the highest quality experience, ensuring full compatibility with all of Sametime's rich features. More importantly, the latest browsers are designed to include better protection against common client-side attacks. Many cross-site scripting (XSS) attacks can be easily neutralized by using a modern web browser. Microsoft's Internet Explorer 8, for example, has a built-in XSS filter. Mozilla's Firefox 3.6.x also includes protection against malicious script execution.

### -Sametime Security Checklist-

- ✓ Passwords are strong
- ✓ SSL connections are required
- ✓ Anonymous access disabled or restricted
- ✓ Latest patches applied to Sametime
- ✓ Latest web browser in use to access Sametime web components

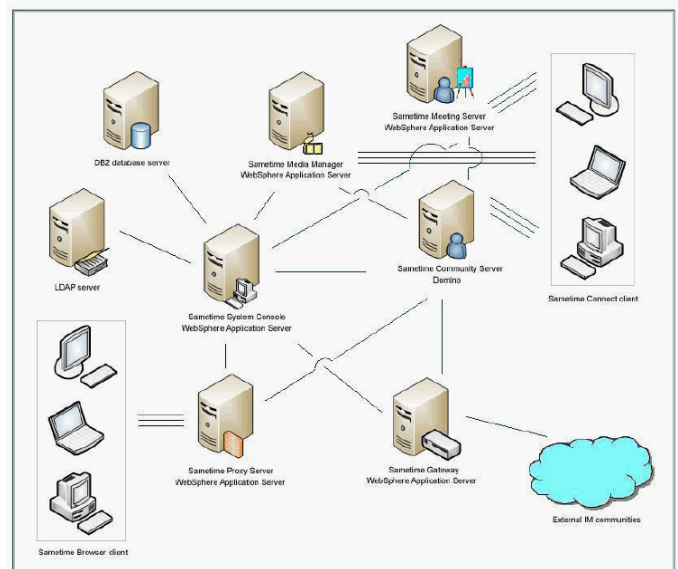
## FIPS 140-2 Compliant

For those organizations who require, or desire, a FIPS 140-2 compliant environment, Lotus Sametime can be configured accordingly. As of this publication, not all Sametime features are FIPS 140-2 compliant, including the IM file transfer and mobility features. Refer to IBM's installation and administration guides for more details.

## Are you Ready?

Deploying a unified communications solution can greatly improve the way employees cooperate and collaborate. This guide has been designed to provide a high-level security reference when deploying a Sametime solution. It is intended to be utilized in parallel with the security features already present in Lotus Domino® and Sametime. There are many configurations for a Sametime deployment. Depending on the feature set desired, the environment can become complex. It is important to implement security throughout the deployment process and work out any bugs along the way. Successfully securing your Sametime environment can save time, money, and help protect your sensitive information from today's most common threats.

The following is a basic Lotus Sametime 8.5.x server deployment.



To obtain full documentation on securing Lotus Sametime, please visit <http://www.ibm.com/support>.

Download a soft copy of this fact sheet from:  
<http://www.nsa.gov/snac>